SURVEILLANCE & COVID-19

THE ISSUE:

In the terrifying, uncertain days following 9/11, Congress authorized measures empowering the most sweeping surveillance the country had ever seen. These measures, the public was assured, were temporary and extraordinary, justified by an emergency that had engulfed the nation.

Nineteen years later, most of those measures are still firmly in place.

Earlier this month, the Department of Health and Human Services (HHS) awarded a contract for a massive new coronavirus-tracking surveillance platform to Palantir – the secretive data mining firm best known for its work with intelligence agencies and law enforcement. The Orwellian-sounding "Protect Now" platform will aggregate data from at least 187 different sources, drawing from the federal government, state and local governments, hospitals and the private sector.

This development should worry all of us. Our existing privacy laws are woefully inadequate to protect the sensitive and personal information that Palantir will analyze. Without adequate privacy protections in place, we run the risk of massive, ongoing government surveillance of all Americans in the name of public health. Without time limitations, that surveillance could become the norm, and the data collected could be used for purposes far beyond the protection of our public health.

First, consider the sheer volume of data that could end up in such a platform. Experts suggest that anywhere from 750,000 tests per week to millions of tests per day may be necessary before the country can be reopened. We don't yet know what information the Palantir platform is tracking, and whether this includes personal testing data – including health data – of any kind. Nor do we know what safeguards, if any, HHS has put place to protect our privacy. Neither HHS nor Palantir has divulged what data goes into the system, how it's used, or with whom it can be shared. These are critical questions the public must have answered.

Second, Palantir's involvement in the tracking and collection data is cause for grave concern: its platforms have previously facilitated grave human rights abuses. The Department of Homeland Security used Palantir technology to arrest over 400 parents, guardians, and other potential caretakers of unaccompanied children in just a month and a half, in a move to deter children from seeking safety by targeting their family members. Another Palantir technology powered the largest immigration raid in a decade, in Mississippi, which led to the arrest of nearly 700 undocumented workers in a poultry plant and tore parents from their children.

Third, there is every reason to suspect that sensitive data collected by Health and Human Services in this context could be coopted by law enforcement. In 2018, the Trump administration inked an information-sharing agreement between Immigration and Customs Enforcement (ICE) and an HHS sub-agency whose mandate is the protection and care of unaccompanied children. The information-sharing agreement permitted ICE to access sensitive information about potential sponsors HHS collected in the family reunification process.

Given this worrisome precedent and the entrenchment of Palantir surveillance technology in federal law enforcement efforts, it is easy to imagine how information collected by this vast new database can potentially be used for ends far beyond its purported objectives.

Widespread testing is, of course, critical: it is essential to the rights to life, health, and even the rights to livelihood and education. Yet while a coordinated, data-driven response to the coronavirus pandemic is critical, neither the government nor private companies like Palantir have carte blanche for unlawful, unnecessary or disproportionate surveillance or data collection, nor should that data be used to achieve ends that do not further public health. Any surveillance related to the pandemic must be justified by legitimate public health needs and limited to only that information necessary to respond to the pandemic. Further, such data collection must be completely transparent and should only last as long as necessary to respond to the pandemic.

TALKING POINTS:

- The Department of Health and Human Services (HHS)'s decision to award a contract for a massive new coronavirus-tracking surveillance platform to Palantir should worry all of us. Our existing privacy laws are woefully inadequate to protect the sensitive and personal information that Palantir will analyze.
- Without adequate privacy protections in place, we run the risk of massive, ongoing government surveillance of all Americans in the name of public health. Without time limitations, that surveillance could become the norm, and the data collected could be used for purposes far beyond the protection of our public health.
- While a coordinated, data-driven response to the coronavirus pandemic is critical, neither the government nor private companies like Palantir have carte blanche for unlawful, unnecessary or disproportionate surveillance or data collection, nor should that data be used to achieve ends that do not further public health.

RECOMMENDATIONS:

- To address these challenges, the White House should:
  - ◊ Be transparent and proactively disclose what information is collected through the Protect Now platform, how this information is used, and who has access to this information
  - ◊ Guarantee that data collected as part of the public health response associated with COVID-19 will only be used for public health purposes, and will not be shared with law enforcement, and in particular ICE
  - ◊ Protect the privacy rights of all Americans by collecting anonymized, aggregated data whenever possible. There should be a legitimate public health justification for any collection of personal health information through the Protect Now platform, and such information should be held only as long as absolutely necessary from a public health perspective.

FOR MORE INFORMATION, PLEASE CONTACT:

Michael Kleinman
Director, Silicon Valley Initiative
(410) 952-6266
Michael.Kleinman@amnesty.org